5

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/788,417	03/01/2004	Yoko Kumagai	64235-017	4957

7590   07/11/2007

MCDERMOTT, WILL & EMERY
600 13th Street, N.W.
Washington, DC 20005-3096

EXAMINER
TABOR, AMARE F

ART UNIT	PAPER NUMBER
2109	

MAIL DATE	DELIVERY MODE
07/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>01 March 2004</u>.

2a)☐ This action is **FINAL**.　　　　2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-7</u> is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-7</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☒ All　b)☐ Some * c)☐ None of:

　　　1.☒ Certified copies of the priority documents have been received.

　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO/SB/08)
　　Paper No(s)/Mail Date <u>03/01/04, 03/02/05 & 11/02/06</u>.

4)☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-7 are examined.

Priority

2.   Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. 10/788,417, filed on 03/01/2004.

Specification

3.   Claim 4 is objected to because of the following informalities: Claim 4, line 3 "he" should be replaced by "the". Appropriate correction is required.

Double Patenting

4.   The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees.   A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claim 1, 4 and 5 are provisionally rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of copending Application No. 11/452,299. Although the conflicting claims are not identical, they are not patentably distinct from each other because both applications claim a public key certificate validation and judging method, comprising: steps of path searching, registration and validation.

This is a <u>provisional</u> obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claim Rejections - 35 USC § 102

5.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.
>
> Claims 1-3, 6 and 7 are rejected under 35 U.S.C. 102(b) as being anticipated by Van Oorschot et

al., (US Patent No.: 6,134,550), referred as "***Van Oorschot***" hereinafter (this reference is cited by the applicant).

6.   *As per claim 1*, Van Oorschot discloses,

        A method for authenticating validity of a public key certificate in compliance with a request, in a validation authority apparatus for certificates, said method comprising: (column 4, lines 37-42, "a **method** and apparatus **for determining validity of a certificate** in a communication system employing trusted paths provides certification path information for a plurality of subscriber units so that each subscriber unit does not need to perform a separate operation of independently reconstructing trusted paths among certificate issuing units").

        - a step of searching for paths (abstract, lines 6-15, "in one embodiment, requesting units, such as certificate validation units or subscribers, send queries to a common certificate chain constructing unit. Each query may identify a beginning and a target certification authority in the community. The certificate chain constructing unit then automatically determines the certification issuing units between the beginning and target certification authorities for each query and **provides certificate chain data** to the requesting unit"). Inherently including a step of searching for paths as claimed.

        - and validating the paths searched for, beforehand; (column 2, lines 22-24, "**certificate chains** correspond to direct trust paths, **also known as certification paths**") and (abstract, lines 15-17, "the requesting unit then performs validity determination on the certificate to be **validated based on the certificate chain data**"). Therefore, the "certificate chains" are "the paths" as claimed. Van Oorschot further discloses that, (column 8, lines 36-39, "if desired, the certificate chain constructing unit 206 may also serve as a client query processor where subscribers are allowed to query for (request) a certificate chain **prior to performing validation**").

        - a path registration step of classifying the paths on the basis of a predetermined criterion in accordance with results of the searches and validations, (column 4, lines 46-51, "depending upon the degree of compilation, a subscriber, certification authority, separate chain constructing server or other entity uses the compiled data as data representing the preferred certificate chain, or **constructs a preferred certificate chain using the certificate chain data**").

Van Oorschot further discloses, (column 8, lines 51-56, "the query signal 402 **may also include some selection criteria data**. The client query processor then reads the certificate chain data 209 and generates a preferred certificate path response signal 404 in response to the query for the requesting certificate validating unit").

- *and registering the classified paths in a database;* (column 5, lines 47-51, "the certificate chain **data storage medium 208 stores certificate chain data 209**, such as a look up table containing entries of data representing trust relationships preferably among all relevant certificate issuing units 202a-202n in a community of interest").

- *and a validity authentication step of receiving the request for authenticating the validity of the public key certificate, from a terminal device,* (column 2, lines 2-7, "since **public key certificates provide a mechanism for obtaining authenticated public keys**, provided the verifier has a trusted verification public key of the certification authority which signed the certificate, trusted paths may be established and maintained among the certification authorities and hence subscribers in large computer networks").

- *and validating the public key certificate by using the paths registered beforehand,* (column 5, lines 23-25, "the requesting unit then performs validity determination on the **certificate to be validated based on the certificate chain data**"). Thus, the "chain data;" i.e., the "paths," as claimed, are used to validate certificates.

7.   _As per claim 2,_ Van Oorschot discloses,

- *wherein: in case where, at the validity authentication step, any valid path corresponding to the validity authentication request is not registered, path search and validation are performed anew, thereby to authenticate the validity of the public key certificate* (see FIG. 6 and column 10, lines 40-48, "the certificate chain-constructing unit 206 then determines whether the end of the chain has been reached as shown in block 604. **If the end of the chain has not been reached**, the certificate chain-constructing unit obtains the associated table entry for the next link from the certificate chain data table 209 as shown in block 606. This link in the chain is then added to the previous link as shown in block 608 and the **process continues until the end of the shortest chain is reached**").

8.   _As per claim 3,_ Van Oorschot discloses,

- *wherein: the predetermined criterion at the path registration step classifies the paths into valid paths and invalid paths in accordance with the results of the validations;* (column 11, lines 61-67, "where the certificate chain data is already in a form that indicates the names of each CA in a shortest trusted path, a querying unit need only obtain the certificate information corresponding to the listed CA's.

Where the certificate chain data includes certificates (or certificate identification data) of the CA's in the shortest trusted path, **the requesting unit need only validate based on the listed certificate information"**).

> *- in case where, at the validity authentication step, a path corresponding to the validity authentication request is registered as the valid path or the invalid path in the database,* (column 6, lines 23-32, "any other suitable types of certificate repositories, for example those accessible via the Lightweight Directory Access Protocol (LDAP) as known in the art, or databases with a standard interface may also be used. As such, certificates of each of these certificate-issuing units are stored therein as are certificate revocation data such as certificate revocation lists (CRL's) and authority revocation lists (ARL's) as known in the art (alternatively, all revoked certificates may be consolidated onto a single list, or recorded among many segmented lists)"). Van Oorschot further discloses, (column 12, lines 1-5, "if desired, the certificate chain constructing unit can also perform the validation process based on the compiled cross-certification data and send a secured **"yes"** or **"no"** response to a requesting unit so that requesting units, such as subscribers, need not perform the chain validation process").

> *- authentication of the validity of the public key certificate is performed in accordance with the registered result* (column 12, lines 5-13, "in such an embodiment, the query may include the target certificate along with a designated start CA (trust anchor). The **chain-constructing unit 206 then performs the validation process and returns response data** representing a "yes" indicating that the target certificate can be trusted, or a "no" indicating that the target certificate cannot be trusted. If desired, a time stamp may also be applied as part of the certificate chain data or other response data").

10.   *As per claim 6,* ejection of claim 3 is incorporated and Van Oorschot further discloses,

> *- step of searching for each path which extends from a trust anchor certificate authority to a certificate authority that issues an end entity certificate;* (see FIG. 3 and column 8, lines 43-47, "the query may take many forms, but preferably indicates data representing **an initial (start) and target (end) certificate issuing unit** and/or it's public key, such as CA1 (FIG. 3) being the starting CA and CA6 being the target or end certificate issuing unit in the path").

> *- step of acquiring and validating a certificate revocation list which concerns the end entity certificate, and which is issued by the certificate authority that issues the pertinent end entity certificate;* (see column 9, lines 37-42, "also, in a system that uses revocation data, if desired, the revocation data from ARL's and CRL's for example, may be **obtained by the certificate validating** unit instead of by the certificate chain data generator 400 so that the subscriber performs the revocation analysis as part of the certificate validating process").

- step of registering the certificate revocation list together with a validation thereof;
(column 9, lines 47-54, "if desired, the certificate chain data generator 400 may also **store certificate revocation data** that it obtained from the directory 302 and transmit the revocation data to the subscriber with the certificate chain data in the query response signal so that the subscriber need not again access the directory 302 or other revocation status checking means such as an on-line status checking server to determine revocation status).

11.   *As per claim 7,* rejection of claim 6 is incorporated and further Van Oorschot discloses,

- in case where, at the validity authentication step, the path corresponding to the validity authentication request is registered as the valid path in the database, (column 8, lines 23-28, "**the certificate chain constructing unit 206 may also digitally sign the certificate chain data** as a trusted entity to assert validity of the certificate chain data for subscribers relying on the certificate chain data so that subscribers or other entities that rely on the certificate chain data may validate that the certificate chain data is trusted").

- it is authenticated without validating the certificate revocation list that the pertinent public key certificate is not revoked (column 8, lines 28-35, "each subscriber would then carry out **conventional validation steps to confirm that the certificate chain data has not expired, has not been revoked** or otherwise rendered untrustworthy. Alternatively, some or all of these steps could be carried out by unit 206, and the subscribing unit could rely upon the digital signature of unit 206 in the chain data as an assurance that these checks have been successful").

Claim Rejections - 35 USC § 103

12.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Van Oorschot as applied to claims 1 ad 3 above, and further in view of Matsuyama et al. (US Patent No: 6,990,583 B2), referred as "*Matsuyama*" hereinafter.

13.   _As per claim 4 and 5,_ Van Oorschot discloses,

         - step of performing path validation in compliance with the validity authentication request,
(see FIG. 6 and column 10, lines 35-48, "the certificate chain constructing unit 206 as shown in block 600
receives subscriber (client) query data such as the name of a start certificate issuing unit and the name of
an target certificate issuing unit. The certificate chain constructing unit 206 then sets the chain to begin at
the start name received in the query as shown in block 602. The **certificate chain-constructing unit 206
then determines whether the end of the chain has been reached** as shown in block 604. If the end of
the chain has not been reached, the certificate chain-constructing unit obtains the associated table entry
for the next link from the certificate chain data table 209 as shown in block 606. This link in the chain is
then added to the previous link as shown in block 608 and the process continues until the end of the
shortest chain is reached").

         **- in case where, at the validity authentication step, the pertinent path corresponding to the
validity authentication request is registered as the valid path;** (column 10, lines 48-55, "an entry in
the certificate chain data 209 look up table includes the CA in the shortest path, data representing the list
of CA's in a shortest path, other paths, more than one path or other data representing a trusted certificate
chain between the start and target CA. As shown in block 610, **data representing the preferred
certificate chain is then generated** and output in the form of response 404 to the requesting unit").

         - step of judging the pertinent path as a valid path (column 10, lines 55-58, "if no certificate
chain data is stored in a relevant entry of the look up table, the client query processor returns a signal
indicating that no trust chain is known corresponding to the query").

         Van Oorschot does not explicitly disclose,
         - constraint item and policy of electronic procedure
         On the other hand, on the same field of endeavor, Matusuyama discloses the above limitation as,
(column 14, lines 15-122, "**name Constraints permitted Subtrees** is a filed indicating the effective range
of a certificate used only when a subject to be certificated is the certificate authority (public-key-certificate
issuer authority). **policy Constraints** describes a specific certificate policy ID corresponding to the
remainder of certificate paths, and a prohibition policy map").

         Therefore, it would have been obvious to one of ordinary skill in the art, at the time the invention
was made, to combine the teachings of Matusuyama to the method of Van Oorschot, because one of
ordinary skill in the art want to form a public key certificate registration authority (see Matusuyama column
8, lines 30-39 and Figs. 6 & 7) efficiently.

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

TITLE: Multi-step digital signature method and system, US 6,209,091 B1
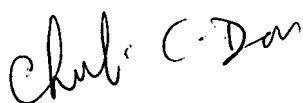
TITLE: Electronic authority server, US 6,073,242

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Amare F. Tabor whose telephone number is (571) 270-3155. The examiner can normally be reached on Mon-Fri 7:30a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Chameli Das can be reached on (571) 270-1392. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AFT

CHAMELI DAS
SUPERVISORY PATENT EXAMINER
7/6/07